KOREAN PATENT ABSTRACT (KR)

Patent Laid-Open Gazette

(51) IPC Code: H04N 7/167
(11) Publication No.: P1999-023602 (43) Publication Date: 25 March 1999
(21) Application No.: 10-1998-033035 (22) Application Date: 14 August 1998

(71) Applicant: LUCENT TECHNOLOGIES INC.

(72) Inventor: Wood Avishy

(54) Title of the Invention: Methods of transmitting, receiving, and decoding encrypted program, and product manufactured based on the same

Abstract:

Provided is a system for transmitting an encryption key used to encode a program together with encrypted program content to a client and restricting access to the transmitted program content. A set-top terminal or a similar mechanism restricts access to transmitted multimedia information using a stored decryption key. The set-top terminal may periodically receive at least one package key SJ from a service provider. Each package key corresponds to a package of a program for which the client has authority for a predetermined period. Each program may be decrypted using a program key KP, which may be unique for the corresponding program, by a head-end server before being transmitted. Header information includes a package pair for each package of the program and is transmitted to the client together with the encrypted program. The package pair may include a program key KP encrypted by a corresponding package key SJ and a package identifier. A particular program p for broadcasting may include a header portion including a package pair for each package of the program and a program portion including the program encrypted using a program key KP. When a client has an authority for a particular program is given to a client, the set-top terminal may decrypt an encrypted program key KP using a stored suitable key SJ. Subsequently, a program key KP can be sued to decrypt the encrypted program. The header information may be interleaved in the program portion or may be transmitted through a separate control channel only therefor.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
H04N 7/167

(11) 공개번호 특1999-023602
(43) 공개일자 1999년03월25일

(21) 출원번호 특1998-033035
(22) 출원일자 1998년08월14일
(30) 우선권주장 8/911,650 1997년08월15일 미국(US)
(71) 출원인 루센트 테크놀러지스 인크
미합중국 뉴저지 머레이 힐 마운틴 애비뉴 600 (우편번호 : 07974-0636)
(72) 발명자 우드 아비샤이
미국 뉴저지주 07039 리빙스톤 펠스우드 드라이브 45
(74) 대리인 김창세, 장성구

실사청구 : 있음

(54) 암호화된 프로그램 송신 및 수신 방법, 복호화 방법 및 제조 물품

요약

본 발명은 프로그램을 암호화하는데 이용된 암호화 키를 암호화된 프로그래밍 내용과 함께 고객에게 송신하고, 송신된 프로그래밍 내용에 엑세스하는 것을 제한하는 시스템을 개시한다. 셋탑 터미널(set-top terminal) 또는 유사한 메커니즘은 저장된 암호 해독 키(decryption keys)를 이용하여 송신된 멀티미디어 정보에 액세스하는 것을 제한한다. 셋탑 터미널은 서비스 제공자로부터 주기적으로 하나 또는 그 이상의 패키지 키 SJ를 수신하는 것이 바람직하며, 각각의 패키지 키는 주어진 주기 동안 고객에게 권한이 주어진 프로그램의 패키지에 대응한다. 각각의 프로그램은 프로그램에 대해 유일할 수도 있는 프로그램 키 KP를 이용하여, 송신하기 전에 헤드엔드 서버에 의해 암호화되는 것이 바람직하다. 헤더 정보는 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍을 포함하며, 암호화된 프로그램과 함께 고객에게 송신된다. 패키지 쌍은 대응 패키지 키 SJ에 의해 암호화된 프로그램 키 KP 뿐만 아니라, 패키지의 식별자도 또한 포함하는 것이 바람직하다. 주어진 프로그램 p의 방송은 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍을 포함하는 헤더 부분과, 프로그램 키 KP를 이용하여 암호화된 프로그램을 포함하는 프로그램 부분으로 구성되는 것이 바람직하다. 고객에게 특정 프로그램에 대해 권한이 부여될 경우, 셋탑 터미널은 저장된 적절한 프로그램 키 SJ를 이용하여 암호화된 프로그램 키 KP를 암호 해독할 수 있으며, 그 후, 암호화된 프로그램을 암호 해독하기 위하여 프로그램 키 KP를 이용할 수 있다. 헤더 정보는 프로그램 부분에 인터리빙되거나 또는, 별개의 전용 제어 채널상에서 송신될 수 있다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명의 일실시예에 따라 암호화된 프로그래밍 내용을 송신하기 위한 시스템을 도시하는 개략적 블럭도.

도 2는 프로그램을 암호화하는데 이용된 암호화 키를 포함하여, 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍과 함께 암호화된 프로그램의 데이터 포맷의 일례에 대한 도면.

도 3은 도 1의 전형적인 헤드엔드 서버에 대한 개략적 블럭도.

도 4는 도 1의 전형적 수신기에 대한 개략적 블럭도.

도 5는 도 4의 프로그램 데이터베이스로부터의 샘플 테이블을 도시하는 도면.

도 6은 도 4의 패키지 데이터베이스로부터의 샘플 테이블을 도시하는 도면.

도 7은 도 5의 인타이틀먼트 데이터베이스로부터의 샘플 테이블을 도시한 도면.

도 8은 도 3의 헤드엔드 서버에 의해 구현되는 전형적인 송신 프로세스를 설명하는 흐름도.

도 9a 및 도 9b는 도 4의 수신기에 의해 구현되는 전형적인 복호화 프로세스를 설명하는 흐름도.

도면의 주요 부분에 대한 부호의 설명

110 : 분배 네트워크 300 : 헤드엔드 서버
310, 410 : 프로세서 320, 420 : 데이터 저장 디바이스

330, 430 : 통신 포트 400, 401 : 셋탑 터미널

500 : 프로그램 데이터베이스 600 : 패키지 데이터베이스

700 : 인타이틀먼트 데이터베이스 800 : 승신 프로세스

900 : 복호화 프로세스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 전반적으로 송신된 프로그래밍 내용에 액세스하는 것을 제한하는 시스템에 관한 것으로, 보다 구체적으로는, 프로그램을 암호화하는데 이용되는 암호화 키(encryption key)와 암호화된 프로그램(encrypted program)을 함께 송신하는 시스템에 관한 것이다.

텔레비전 시청자가 이용할 수 있는 채널의 수가 그러한 채널상에서 이용할 수 있는 프로그래밍 내용의 다양성과 함께 증가함에 따라, 케이블 텔레비전 조작자 및 디지털 위성 서비스 조작자와 같은 서비스 제공자가 텔레비전 시청자들의 대다수를 만족시키는 채널 및 프로그램의 패키지(packages)를 제공하는 것이 점증적으로 요구되었다. 고객에게 제공될 수 있는 패키지의 개발은 일반적으로 마케팅 기능이다. 일반적으로, 서비스 제공자는 단일 프로그램에서부터 모든 프로그램까지의 여러 크기의 패키지와, 이들 사이의 여러 조합을 제공하기를 원한다.

서비스 제공자는 대체로, 종종 헤드엔드(head-end)라고 하는 송신기로부터 다수의 고객에게 텔레비전 프로그램을 방송한다. 각각의 고객에게는 대체로, 구입된 패키지와 관련된 수신된 프로그래밍의 서브셋(subset)에만 권리가 부여된다. 무선 방송 환경에서, 예를 들면, 송신된 프로그래밍은 안테나 또는 위성 접시형 안테나와 같은 적절한 수신기를 이용하여 누구든지 수신할 수 있다. 따라서, 송신된 프로그램에 액세스하는 것을 필요한 패키지를 구입한 허가된 고객에게 한정하기 위하여, 서비스 제공자는 대체로 송신된 프로그램을 암호화하고, 고객에게 권한이 부여된 프로그램을 암호 해독하는데 이용될 수도 있는 하나 또는 그 이상의 암호 해독 키를 포함하는 셋탑 터미널(STT; a set-top terminal)을 고객에게 제공한다. 이러한 방식으로, 셋탑 터미널은 암호화된 송신을 수신하고, 고객에게는 권한이 부여되지만 그 외에는 권한이 부여되지 않는 프로그램을 암호 해독한다.

저장된 암호 해독 키를 포함하여 셋탑 터미널에 저장된 고감도 정보의 저작권 침해를 최소화하기 위하여, 셋탑 터미널은 대체로 보안 프로세서와, 암호 해독 키를 저장하기 위해 수 킬로 비트 정도의 용량을 갖는 보안 메모리를 포함한다. 보안 메모리는 보통 비휘발성이며 함부로 조작할 수 없다. 또한, 예를 들면, 각각의 빌링 주기(billing period) 동안 키를 원하는 대로 재프로그래밍 할 수 있도록, 보안 메모리는 기록 가능한 것이 바람직하다. 종래의 셋탑 터미널의 보안 메모리 용량이 제한됨으로써, 저장될 수 있는 키의 수가 제한되어 서비스 제공자에 의해 제공될 수 있는 패키지의 수가 제한된다. 대체로 월간 빌링 주기 동안 서비스 제공자에 의해 방송되는 프로그램의 수는 200,000 개 정도일 수 있음을 알 수 있다.

한 가지 변경에서, 종래의 셋탑 터미널은 서비스 제공자에 의해 제공되는 프로그램의 각각의 패키지(package)에 대응하는 비트 엔트리(bit entry)를 갖는 비트 벡터를 포함한다. 대체로, 각각의 패키지는 하나의 텔레비전 채널에 대응한다. 특정 고객에게 하나의 패키지에 대한 권한이 부여될 경우, 셋탑 터미널에 저장된 비트 벡터에 있어서의 대응 비트 엔트리는 1로 세팅된다. 그 후, 서비스 제공자에 의해 송신된 모든 프로그램은 단일 키를 이용하여 암호화된다. 소정의 프로그램을 수신하면, 셋탑 터미널은 대응 비트 엔트리가 세팅되었는가를 결정하기 위하여 비트 벡터에 액세스 한다. 비트 엔트리가 세팅되었을 경우, 셋탑 터미널은 프로그램을 암호 해독하기 위하여 저장된 단일 암호 해독 키를 이용한다.

이론상으로, 각각의 프로그램용 비트 엔트리를 제공함으로써 비트 벡터 방식(bit vector scheme)에서 융통성이 생기는 반면, 단일 빌링 주기에서 많은 프로그램을 송신하는 시스템에서는 비트 벡터의 길이가 비실용적일 것이다. 또한, 그러한 시스템에서의 액세스 제어는 비트 벡터에서의 엔트리에 의해 배타적으로 제공되며 암호화에 의한 것이 아니다. 따라서, 고객이 비트 벡터를 오버라이트(overwrite)할 수 있고 모든 비트를 1로 세팅할 경우, 고객은 모든 프로그램에 액세스할 수 있다.

다른 변경에 있어서, 프로그램은 패키지로 분할되고, 주어진 패키지에서 모든 프로그램은 동일한 키를 이용하여 암호화된다. 또한, 각각의 패키지는 대체로 하나의 텔레비전 채널에 대응한다. 셋탑 터미널은 고객에게 권한이 부여되는 각각의 패키지에 대한 암호 해독 키를 저장한다. 따라서, 하나의 프로그램이 다수의 패키지에 포함될 경우, 프로그램은 각각의 관련 패키지에 대하여 재송신되어야 하며, 각각의 송신은 특수 패키지에 대응하는 암호화 키를 이용하여 암호화된다. 액세스 제어가 암호화에 의한 것일지라도, 주어진 프로그램을 여러 번 재송신하는 것과 관련된 오버헤드는 서비스 제공자가 동일한 프로그램을 다수의 패키지에 배치하는 것을 방해하며, 프로그램의 패키지를 설계시 융통성을 제한한다.

프로그래밍 내용을 암호화하여 송신하는 이전의 시스템이 권한이 부여된 고객에게 액세스하는 것을 제한함에 있어서는 비교적 성공적이었지만, 그와 같은 이전의 시스템은 셋탑 터미널의 보안 메모리의 제한된 용량을 초과하지 않고서, 텔레비전 네트워크와 같은 서비스 제공자가 다수의 프로그램을 포함하는 상이한 여러 패키지를 고객에게 제공할 수는 없다. 암호화된 프로그래밍 내용을 송신하기 위한 종래의 시스템에 관하여 위에서 설명된 단점에서 명백한 바와 같이, 프로그램을 암호화하는데 이용되는 유일한 키와 함께, 유일한 키를 이용하여 암호화된 프로그램을 송신하는 시스템이 필요하다. 서비스 제공자가 각각의 패키지에 대한 프로그램을 재송신할 필요없이, 다수의 패키지에 하나의 프로그램을 포함시킬 수 있는 시스템이 더 필요하다. 송신된 프로그래밍 내용과 관련된 오버헤드를 크게 증가시키지 않으면서 셋탑 터미널의 보안 메모리에 제한을 받지 않는 액세스 제어 시스템이 더 필요하다.

발명이 이루고자 하는 기술적 과제

일반적으로, 암호화된 프로그래밍 내용은 송신기 또는 헤드엔드 서버(head-end server)를 이용하여 서비스 제공자에 의해 하나 또는 그 이상의 고객에게 송신된다. 본 발명의 한가지 양상에 따르면, 프로그램을 암호화하는데 이용된 암호화 키는 프로그래밍 내용과 함께 고객에게 송신된다. 각각의 고객은 암호 해독 키를 이용하여, 송신된 멀티미디어 정보에 액세스하는 것을 제한하는 셋탑 터미널 또는 다른 메커니즘을 갖는 것이 바람직하다. 본 발명의 또다른 양상에 따르면, 셋탑 터미널은 헤드엔드로부터 주기적으로 하나 또는 그 이상의 패키지 키 SJ를 수신하는 것이 바람직하며, 각각의 패키지 키는 고객에게 주어진 주기 동안 권한이 부여된 프로그램의 패키지에 대응한다.

각각의 프로그램은 프로그램에 대해 유일할 수도 있는 프로그램 키 KP를 이용하여, 송신하기 전에 헤드엔드 서버에 의해 암호화되는 것이 바람직하다. 헤드엔드 서버는 암호화된 프로그램을 송신할 뿐만 아니라, 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍을 포함하며, 헤더 정보(header information)를 고객에게 송신하는 것이 바람직하다. 패키지 쌍은 대응 패키지 키 SJ에 의해 암호화된 프로그램 키 KP 뿐만 아니라, 패키지의 식별자도 또한 포함하는 것이 바람직하다. 따라서, 일실시예에서, 주어진 프로그램 p의 방송은 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍을 포함하는 헤더 부분과, 프로그램 키 KP를 이용하여 암호화된 프로그램을 포함하는 프로그램 부분으로 구성된다. 이러한 방식으로, 고객이 특정 프로그램에 대해 권한을 부여받을 경우, 셋탑 터미널은 저장된 적절한 패키지 키 SJ를 이용하여 암호화된 프로그램 키 KP를 암호 해독할 수 있고, 그 후 암호화된 프로그램을 암호 해독하기 위하여 프로그램 키 KP를 이용할 수 있을 것이다. 여러 실시예에서, 헤더 정보는 프로그램 부분과 인터리빙되거나(interleaved) 또는 개별 전용 제어 채널상에서 송신될 수 있다.

이하의 상세한 설명 및 도면을 참조함으로써, 본 발명의 또다른 특징 및 이점을 알 수 있을 뿐만 아니라, 본 발명을 보다 완전하게 이해할 수 있을 것이다.

발명의 구성 및 작용

도 1은 헤드엔드 서버(300)와 같은 송신기를 이용하는 서비스 제공자로부터 하나 또는 그 이상의 분배 네트워크(110)를 통하여 셋탑 터미널(400)과 같은 셋탑 터미널(400-401)을 구비하는 하나 또는 그 이상의 고객에게 비디오, 오디오 및 데이터와 같은 암호화된 멀티미디어 정보를 송신하는 예시적인 네트워크 환경을 도시한다. 본 명세서에서 이용된 바와 같이, 셋탑 터미널은 예를 들면, 원격 통신 장비 뿐만 아니라 컴퓨터 구성도 포함하는, 암호 해독 키를 이용하여 송신된 멀티미디어 정보에 액세스하는 것을 제한하는 어떠한 메커니즘도 포함한다. 셋탑 터미널에 의해 실행되는 소프트웨어가 서비스 제공자에 의해 다운로드될 수 있다. 분배 네트워크(110)는 디지털 위성 서비스(DSS□SYMBOL 212\fSymbol□)와 같은 프로그래밍 내용의 분배를 위한 무선 방송 네트워크나 또는, 케이블 텔레비젼 네트워크(CATV), 공중 회선 교환 전화망(PSTN; Public Switched Telephone Network), 광 네트워크, 광대역 종합 정보 통신망(ISDN; integrated services digital network) 또는 인터넷과 같은 종래의 배선식 네트워크(wired network)일 수 있다.

본 발명의 특성에 따라, 셋탑 터미널(400)은 도 3과 함께 이하에 더 기술된 헤드엔드 서버(300)로부터 하나 또는 그 이상의 패키지 키 SJ를 간헐적으로 수신하며, 각각의 패키지 키는 빌링 주기와 같은 주어진 시간 간격 동안 고객에게 권한이 부여된 패키지에 대응한다. 본 명세서에서 이용된 바와 같이, 패키지는 미리 정해진 프로그램 세트이며, 주어진 프로그램이 하나 또는 그 이상의 패키지에 속할 수 있다. 프로그램은 텔레비젼 에피소드(television episode) 또는 영화와 같은 특정 길이의 어떠한 연속 멀티미디어 송신일 수도 있다. 패키지 키 SJ는 통상의 기술을 가진 자에 의해 명백한 바와 같이, 어떠한 적절한 보안 단방향 또는 양방향의 프로토콜이라도 이용하여 헤드엔드 서버(300)로부터 셋탑 터미널(400)로 다운로드될 수 있다.

이하에 더 기술된 바와 같이, 송신된 프로그램 각각은 프로그램에 대해 유일할 수도 있는 프로그램 키 KP를 이용하여 헤드엔드 서버(300)에 의해 암호화된다. 적절한 암호화 및 보안 기술에 대한 상세한 검토를 위하여, 본 명세서에서 인용된 B. Schneier, Applied Cryptography(2d ed. 1997)를 참조하자. 헤드엔드 서버(300)는 또한 암호화된 프로그램을 송신할 뿐만 아니라, 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍을 포함하여, 헤더 정보를 셋탑 터미널(400)에 송신한다. 패키지 쌍은 대응 패키지 키 SJ에 의해 암호화된 프로그램 키 KP 뿐만 아니라, 패키지의 식별자도 또한 포함한다.

따라서, 도 2에 도시된 바와 같이, 주어진 프로그램 p의 방송은 프로그램이 속하는 각각의 패키지에 대한 패키지 쌍(230)을 포함하는 헤더 부분(210)과, 프로그램 키 KP를 이용하여 암호화된 프로그램을 포함하는 프로그램 부분(220)으로 구성된다. 이러한 방식으로, 고객에게 특정 프로그램에 대한 권한이 부여될 경우, 셋탑 터미널(400)은 저장된 적절한 패키지 키 SJ을 이용하여 암호화된 프로그램 키 KP를 암호 해독할 수 있고, 그 후, 암호화된 프로그램을 암호 해독하기 위하여 프로그램 키 KP를 이용할 수 있다.

도 3은 예시적인 헤드엔드 서버(300)의 구성을 도시하는 블럭도이다. 헤드엔드는 텔레비젼 네트워크, 케이블 조작자, 디지털 위성 서비스 조작자 또는 암호화된 프로그래밍 내용을 송신하는 어떠한 서비스 제공자와도 관련될 수도 있다. 헤드엔드 서버(300)는 예를 들면, 본 명세서에서 본 발명의 기능과 동작을 실행하도록 수정되고 IBM사에 의해 제조된 RS 6000 서버로서 구현될 수도 있다. 헤드엔드 서버(300)는 프로세서(310)와, 가령 데이터 저장 디바이스(320)와 같은 관련 메모리를 포함하는 것이 바람직하다. 프로세서(310)는 단일 프로세서나 또는 병렬로 동작하는 다수의 프로세서로서 구현될 수도 있다. 데이터 저장 디바이스(320) 및/또는 판독 전용 메모리(ROM)는 프로세서(310)가 검색하고 해석하여 실행하도록 동작할 수 있는 하나 또는 그 이상의 명령을 저장하도록 동작할 수 있다. 프로세서(310)는 알려진 방식으로 제어 장치, 산술 논리 연산 장치(ALU; arithmetic logic unit) 및 가령 예를 들면, 명령 캐시 또는 다수의 레지스터와 같은 국부 메모리 저장 디바이스를 포함하는 것이 바람직하다. 제어 장치는 데이터 저장 디바이스(320) 또는 ROM으로부터의 명령을 검색하도록 동작할 수 있다. ALU는 명령을 실행하는데 필요한 다수의 동작을 실행하도록 동작할 수 있다. 국부 메모리 저장 디바이스는 일시적 결과와 제어 정보를 저

장하기 위해 이용된 고속 저장 장치를 제공하도록 동작할 수 있다.

도 5 및 도 6과 함께 이하에 더 기술된 바와 같이, 데이터 저장 디바이스(320)는 프로그램 데이터베이스(500) 및 패키지 데이터베이스(600)를 포함하는 것이 바람직하다. 프로그램 데이터베이스(500)는 프로그램이 속하는 패키지와 대응 프로그램 키 KP를 포함하며, 예를 들면, 주어진 빌링 주기 동안 헤드엔드 서버에 의해 송신될 각각의 프로그램 p에 관한 정보를 저장한다. 패키지 데이터베이스(600)는 각각의 패키지의 명칭과 대응 패키지 키 SJ를 포함하여, 헤드엔드 서버(300)에 의해 고객에게 제공되는 각각의 패키지에 관한 정보를 저장하는 것이 바람직하다.

또한, 도 8과 함께 이하에 더 기술된 바와 같이, 데이터 저장 디바이스(320)는 송신 프로세스(800)를 포함하는 것이 바람직하다. 일반적으로, 송신 프로세스(800)는 암호화된 프로그램과 함께 송신될 패키지 쌍을 생성하기 위하여, 주어진 프로그램의 프로그램 키 KP와, 그 프로그램이 속하는 패키지를 식별한다. 통신 포트(330)는 헤드엔드 서버(300)를 분배 네트워크(110)에 접속함으로써, 헤드엔드 서버(300)를 도 1에 도시된 셋탑 터미널(400)과 같은 각각의 접속된 수신기에 연결한다.

도 4는 예시적인 셋탑 터미널(400)의 구조를 도시하는 블럭도이다. 셋탑 터미널(400)은 예를 들면, 본 발명의 기능과 동작을 실행하도록 본 명세서에서 수정되고 General Instruments사로부터 구입할 수 있는 셋탑 터미널(STT; set-top terminal)과 같이 텔레비전과 관련된 셋탑 터미널로서 구현될 수도 있다. 셋탑 터미널(400)은 도 3과 함께 위에서 설명된 하드웨어와 유사한 방식으로 동작하는 통신 포트(430) 뿐만 아니라, 프로세서(410)와, 데이터 저장 디바이스(420)와 같은 관련 메모리도 포함하는 것이 바람직하다.

도 7과 함께 이하에 더 기술된 바와 같이, 데이터 저장 디바이스(420)는 인타이틀먼트 데이터베이스(700)를 포함하는 것이 바람직하다. 인타이틀먼트 데이터베이스(700)는 데이터 저장 디바이스(420)의 보안 부분에 저장되는 것이 바람직하다. 인타이틀먼트 데이터베이스(700)는 고객에게 권한이 부여되는 각각의 패키지에 대한 패키지 식별자와 대응 패키지 키 SJ를 저장하는 것이 바람직하다. 또한, 도 9a 및 9b와 함께 이하에 더 기술된 바와 같이, 데이터 저장 디바이스(420)는 복호화 프로세스(900)를 포함하는 것이 바람직하다. 일반적으로, 복호화 프로세스(900)는 송신된 프로그램 키 KP를 암호 해독하기 위하여 저장된 대응 패키지 키 SJ를 이용하고 프로그램을 암호 해독하기 위하여 프로그램 키 KP를 이용함으로써 고객에게 권한이 부여된 프로그램을 암호 해독한다.

도 5는 프로그램이 속하는 패키지와 대응 프로그램 키 KP를 포함하여, 예를 들면, 주어진 빌링 주기 동안 헤드엔드 서버(300)에 의해 송신될 각각의 프로그램 p에 관한 정보를 저장하는 것이 바람직한 전형적인 프로그램 데이터베이스(500)를 도시한다. 프로그램 데이터베이스(500)는 각각 상이한 프로그램과 관련된 가령 레코드(505-520)와 같은 다수의 레코드를 유지한다. 필드(525)에서 프로그램 명칭에 의해 식별되는 각각의 프로그램의 경우, 프로그램 데이터베이스(500)는 필드(530)에서 프로그램이 속하는 대응 패키지의 표시와 필드(535)에서 대응 프로그램 키 KP를 포함한다.

도 6은 패키지 각각의 명칭과 대응 패키지 키 SJ를 포함하여, 헤드엔드 서버(300)에 의해 고객에게 제공되는 각각의 패키지에 관한 정보를 저장하는 것이 바람직한 전형적인 패키지 데이터베이스(600)를 도시한다. 패키지 데이터베이스(600)는 상이한 패키지와 각각 관련된 레코드(605-640)와 같은 다수의 레코드를 유지한다. 필드(650)에서 패키지 식별자에 의해 식별된 각각의 패키지의 경우, 패키지 데이터베이스(600)는 필드(660)에서 대응 패키지 명칭의 표시와, 필드(670)에서 대응 패키지 키 SJ를 포함한다.

도 7은 고객에게 권한이 부여된 각각의 패키지에 대한 패키지 식별자와 대응 패키지 키 SJ를 저장하는 것이 바람직한 전형적인 인타이틀먼트 데이터베이스(700)를 도시한다. 인타이틀먼트 데이터베이스(700)는 권한이 부여된 상이한 패키지와 각각 관련된 가령 레코드(710-720)와 같은 다수의 레코드를 유지한다. 필드(725)에서 패키지 식별자에 의해 식별된 각각의 패키지의 경우, 인타이틀먼트 데이터베이스(700)는 필드(735)에서 대응 패키지 키 SJ의 표시를 포함한다.

전술한 바와 같이, 헤드엔드 서버(300)는 암호화된 프로그램과 함께 송신될 패키지 쌍을 생성하기 위하여, 주어진 프로그램의 프로그램 키 KP와 프로그램이 속하는 패키지를 식별하고 도 8에 도시된 송신 프로세스(800)를 실행하는 것이 바람직하다. 실제 송신 단계와는 다른 송신 프로세스(800)는 오프라인(offline)으로 실행되거나 또는 실시간으로 실행될 수 있음을 알 수 있다. 도 8에 도시된 바와 같이, 송신 프로세스(800)는 송신될 프로그램을 식별함으로써 단계(810) 동안 본 발명의 원리를 구현하는 프로세스를 시작한다.

그 후, 송신 프로세스(800)는 단계(820) 동안 프로그램 데이터베이스(500)로부터 프로그램에 대응하는 프로그램 키 KP와 프로그램이 속하는 패키지의 리스트를 검색한다. 프로그램이 속하는 각각의 패키지의 경우, 송신 프로세스(800)는 송신된 헤더 정보에 포함될 패키지 쌍을 생성하기 위하여, 패키지 데이터베이스(600)로부터 패키지 식별자와 대응 패키지 키 SJ를 검색할 것이다.

프로그램은 그 후 단계(820) 동안 검색된 프로그램 키 KP를 이용하여 단계(840) 동안 암호화될 것이다. 끝으로, 송신 프로세스(800)는 프로그램 제어가 단계(860) 동안 종료하기 전에, 단계(850) 동안 패키지 쌍의 세트와 함께 암호화된 프로그램을 송신할 것이다. 패키지 쌍을 포함하는 헤더 정보는 프로그램 정보의 송신을 통하여 주기적으로 인터리빙되어, 고객이 프로그램 동안 채널을 변경할 수 있고 프로그램을 암호 해독하는데 필요한 송신된 키를 얻을 수 있는 것이 바람직하다. 헤더 정보를 주기적으로 송신함으로써 초래된 오버헤드(overhead)는 요구된 암호 해독 키가 얻어질 때까지 채널을 변경한 후 고객이 유발할 지연에 대하여 평형을 이루어야 한다. 또다른 실시예에서, 패키지 쌍을 포함하는 헤더 정보는 바커 채널(Barker channel)과 같은 별개의 제어 채널상에서 연속적으로 송신될 수 있다.

전술한 바와 같이, 셋탑 터미널(400)은 도 9a 및 9b에 도시된 복호화 프로세스(900)를 실행하여, 송신된 프로그램 키 KP를 암호 해독하기 위하여 저장된 대응 패키지 키 SJ를 이용하고 프로그램을 암호 해독하기 위하여 프로그램 키 KP를 이용함으로써 고객에게 권한이 부여된 프로그램을 암호 해독한다. 도 9a에 도시된 바와 같이, 복호화 프로세스(900)는 특정 채널로 돌리기 위한 고객 명령을 수신하면 단계(910) 동안 본 발명의 원리를 구현하는 프로세스를 시작한다.

그 후, 셋탑 터미널(400)은 단계(920) 동안 요구된 채널로 돌려서 적절한 신호를 수신할 것이다. 복호화 프로세스(900)는 그런 다음에, 요구된 채널상에서 송신된 프로그램에 대하여 단계(930) 동안 송신된 패키지 쌍을 검색한다. 그런 다음, 요구된 프로그램을 포함하는 패키지에 대해 고객에게 권한이 부여되는가의 여부를 결정하기 위하여, 단계(940) 동안 테스트가 실행된다. 예를 들면, 복호화 프로세스(900)는 단계(930) 동안 검색된 패키지 쌍 중 하나로부터의 패키지 식별자가 인타이틀먼트 데이터베이스(700)에 저장된 패키지 식별자와 매칭하는가의 여부를 결정할 것이다.

요구된 프로그램을 포함하는 패키지에 대해 고객에게 권한이 부여되지 않음을 단계(940) 동안 결정할 경우, 프로그램 제어가 단계(960) 동안 종료하기 전에 선택된 프로그램을 시청할 권한이 고객에게 주어지지 않음을 나타내는 메시지가 단계(950) 동안 고객에게 송신되는 것이 바람직하다. 그러나 요구된 프로그램을 포함하는 패키지에 대해 고객에게 권한이 부여됨이 단계(940) 동안 결정될 경우, 프로그램 제어는 단계(970)(도 9b)로 진행한다.

요구된 프로그램을 시청할 권한이 고객에게 부여될 경우, 복호화 프로세스(900)는 단계(970) 동안 인타이틀먼트 데이터베이스(700)로부터 권한이 부여된 패키지에 대응하는 패키지 키 SJ를 검색하고, 단계(980) 동안 검색된 패키지 키 SJ를 이용하여, 송신된 헤더 정보에 포함되거나 또는 별개의 제어 채널상의 송신된 프로그램 키를 암호 해독한다. 끝으로, 프로그램 그 자체는 프로그램 제어가 단계(995) 동안 종료하기 전에 단계(990) 동안 프로그램 키 KP를 이용하여 단계(990) 동안 암호 해독된다.

복호화 프로세스(900)는 전술한 바와 같이, 송신된 암호 해독 키를 얻고 요구된 채널에 대해 고객에게 권한이 부여되는가의 여부를 결정하도록 시도하기 전에, 고객이 특정 채널을 요구하도록 대기할 수 있으며, 또는, 데이터 저장 디바이스(420)에 저장하기 위한 송신된 패키지 쌍을 얻고 고객의 인타이틀먼트를 사전 결정하기 위하여 모든 채널을 교번적으로 주기적으로 주사할 수 있다.

본 명세서에서 도시되고 기술된 실시예 및 변경은 단지 본 발명의 원리를 예시하는 것이며, 본 발명의 영역과 정신을 벗어나지 않고서도, 당업자에 의해 여러 가지 수정이 구현될 수 있음을 알아야 한다.

발명의 효과

본 발명에 따른 암호화된 프로그램 송신 및 수신 방법, 복호화 방법 및 제조 물품에 의하면, 프로그램을 암호화하는데 이용되는 암호화 키와 암호화된 프로그램을 함께 송신하는 시스템이 제공된다.

(도) 청구의 범위

청구항 1

최종 사용자에게 제한적으로 액세스할 수 있는 다수의 프로그램을 송신하는 방법에 있어서,

① 다수의 패키지-각각의 패키지는 상기 프로그램 중 적어도 하나의 프로그램을 포함함-를 정의하는 단계와,

② 상기 최종 사용자에 의해 획득된 각각의 패키지에 대한 패키지 키를 상기 최종 사용자에게 제공하는 단계와,

③ 프로그램 키를 이용하여 상기 최종 사용자에게 송신될 프로그램을 암호화하는 단계와,

④ 상기 프로그램이 속하는 각각의 패키지에 대한 패키지 정보와 함께 상기 암호화된 프로그램을 송신하는 단계-상기 패키지 정보는 상기 패키지 키에 의해 암호화된 상기 프로그램 키를 포함함-

를 포함하는 프로그램 송신 방법.

청구항 2

제 1 항에 있어서,

상기 패키지 정보는 상기 관련 패키지의 식별자를 더 포함하는 프로그램 송신 방법.

청구항 3

제 1 항에 있어서,

상기 패키지 정보는 상기 암호화된 프로그램의 송신에 의해 인터리빙되는 프로그램 송신 방법.

청구항 4

제 1 항에 있어서,

상기 패키지 정보는 제어 채널상에서 송신되는 프로그램 송신 방법.

청구항 5

프로그램의 적어도 하나의 패키지와 관련된 프로그램을 다수의 고객에게 송신하는 방법에 있어서,

① 상기 고객에 의해 획득된 각각의 패키지에 대한 패키지 키를 상기 각각의 고객에게 제공하는 단계와,

② 상기 프로그램과 관련된 상기 패키지를 식별하는 단계와,

③ 프로그램 키를 이용하여 상기 고객에게 송신될 상기 프로그램을 암호화하는 단계와,

④ 식별된 각각의 패키지에 대한 패키지 정보-상기 패키지 정보는 상기 패키지 키에 의해 암호화된 상기

프로그램 키를 포함함-와 함께 상기 암호화된 프로그램을 송신하는 단계

를 포함하는 프로그램 송신 방법.

청구항 6

제 5 항에 있어서,

상기 패키지 정보는 상기 관련된 패키지의 식별자를 더 포함하는 프로그램 송신 방법.

청구항 7

제 5 항에 있어서,

상기 패키지 정보는 상기 암호화된 프로그램의 송신에 의해 인터리빙되는 프로그램 송신 방법.

청구항 8

제 5 항에 있어서,

상기 패키지 정보는 제어 채널상에서 송신되는 프로그램 송신 방법.

청구항 9

프로그램의 적어도 하나의 패키지와 관련된 프로그램을 다수의 고객에게 송신하는 방법에 있어서,

① 프로그램 키를 이용하여 상기 프로그램을 암호화하는 단계와,

② 상기 암호화된 프로그램과 함께 상기 프로그램 키를 상기 고객에게 송신하는 단계

를 포함하는 프로그램 송신 방법.

청구항 10

제 9 항에 있어서,

상기 프로그램 키는 상기 프로그램이 관련된 각각의 패키지에 대한 패키지 키에 의해 암호화되어 송신되는 프로그램 송신 방법.

청구항 11

제 9 항에 있어서,

하나 또는 그 이상의 패키지 키를 각각의 고객에게 송신하는 단계를 더 포함하되, 각각의 패키지 키는 상기 고객에게 권한이 부여되는 프로그램의 패키지에 대응하는 프로그램 송신 방법.

청구항 12

제 9 항에 있어서,

상기 프로그램 키는 상기 암호화된 프로그램의 송신에 의해 인터리빙되는 프로그램 송신 방법.

청구항 13

제 9 항에 있어서,

상기 프로그램 키는 제어 채널상에서 송신되는 프로그램 송신 방법.

청구항 14

프로그램의 패키지와 관련된 암호화된 프로그램을 복호화하기 위한 방법에 있어서,

① 패키지 정보-상기 패키지 정보는 패키지 키에 의해 암호화된 프로그램 키를 포함하고, 상기 프로그램 키는 상기 프로그램을 암호화하기 위하여 상기 프로그램의 제공자에 의해 이용됨-와 함께 상기 암호화된 프로그램을 수신하는 단계와,

② 상기 패키지에 대응하는 패키지 키를 검색하는 단계와,

③ 상기 프로그램 키를 획득하기 위해 상기 검색된 패키지 키를 이용하여 상기 패키지 정보를 암호 해독하는 단계와,

④ 상기 프로그램 키를 이용하여 상기 암호화된 프로그램을 암호 해독하는 단계

를 포함하는 암호화된 프로그램 복호화 방법.

청구항 15

제 14 항에 있어서,

상기 제공자로부터 하나 또는 그 이상의 패키지 키를 수신하는 단계를 더 포함하되, 각각의 패키지 키는 고객에게 권한이 부여된 프로그램의 패키지에 대응하는 암호화된 프로그램 복호화 방법.

청구항 16

제 14 항에 있어서,

상기 패키지 정보는 상기 관련된 패키지의 식별자를 더 포함하는 암호화된 프로그램 복호화 방법.

청구항 17

제 14 항에 있어서,

상기 패키지 정보는 상기 암호화된 프로그램의 송신에 의해 인터리빙되는 암호화된 프로그램 복호화 방법.

청구항 18

제 14 항에 있어서,

상기 패키지 정보는 제어 채널상에서 송신되는 암호화된 프로그램 복호화 방법.

청구항 19

제 14 항에 있어서,

상기 패키지 정보는 상기 프로그램에 대한 시청 요구시 평가되는 암호화된 프로그램 복호화 방법.

청구항 20

제 14 항에 있어서,

상기 패키지 정보는 상기 프로그램에 대한 시청 요구에 앞서 평가되는 암호화된 프로그램 복호화 방법.

청구항 21

제한적으로 액세스할 수 있는 암호화된 프로그램을 수신하는 방법에 있어서,

① 상기 고객에게 권한이 부여된 상기 프로그램의 각각의 패키지에 대응하는 패키지 키를 저장하는 단계와,

② 패키지 정보-상기 패키지 정보는 상기 패키지 키에 의해 암호화된 프로그램 키를 포함하고, 상기 프로그램 키는 상기 프로그램을 암호화하기 위하여 상기 프로그램의 제공자에 의해 이용됨-와 함께 상기 암호화된 프로그램을 수신하는 단계와,

③ 프로그램 키를 획득하기 위하여 상기 수신된 패키지 키를 이용하여 상기 패키지 정보를 암호 해독하는 단계와,

④ 상기 프로그램 키를 이용하여 상기 암호화된 프로그램을 암호 해독하는 단계

를 포함하는 프로그램 수신 방법.

청구항 22

제 21 항에 있어서,

상기 패키지 정보는 상기 관련된 패키지의 식별자를 더 포함하는 프로그램 수신 방법.

청구항 23

제 21 항에 있어서,

상기 패키지 정보는 상기 암호화된 프로그램의 송신에 의해 인터리빙되는 프로그램 수신 방법.

청구항 24

제 21 항에 있어서,

상기 패키지 정보는 제어 채널상에서 송신되는 프로그램 수신 방법.

청구항 25

제 21 항에 있어서,

상기 패키지 정보는 상기 고객이 상기 프로그램에 대한 시청 요구시 평가되는 프로그램 수신 방법.

청구항 26

제 21 항에 있어서,

상기 패키지 정보는 상기 고객이 상기 프로그램에 대한 시청 요구에 앞서 평가되는 프로그램 수신 방법.

청구항 27

제조 물품에 있어서,

컴퓨터 판독 가능한 매체(computer readable medium)상에 구현된 컴퓨터 판독 가능한 코드 수단을 구비하는 컴퓨터 판독 가능한 매체를 포함하되,

상기 컴퓨터 판독 가능한 프로그램 코드 수단은

⑧ 송신될 프로그램과 관련된 하나 또는 그 이상의 패키지-상기 패키지 각각은 관련된 패키지 키를 구비

합-를 식별하는 단계와,

ⓑ 프로그램 키를 이용하여 다수의 고객에게 송신될 상기 프로그램을 암호화하는 단계와,

ⓒ 식별된 각각의 패키지에 대한 패키지 정보-상기 패키지 정보는 상기 패키지 키에 의해 암호화된 상기 프로그램 키를 포함함-와 함께 상기 암호화된 프로그램을 송신하는 단계

를 포함하는 제조 물품.

청구항 28

제조 물품에 있어서,

컴퓨터 판독 가능한 매체상에 구현된 컴퓨터 판독 가능한 코드 수단을 구비하는 컴퓨터 판독 가능한 매체를 포함하되,

상기 컴퓨터 판독 가능한 프로그램 코드 수단은

ⓐ 패키지 정보-상기 패키지 정보는 패키지 키에 의해 암호화된 프로그램 키를 포함하며, 상기 프로그램 키는 상기 프로그램을 암호화하는데 이용됨-와 함께 암호화된 프로그램을 수신하는 단계와,

ⓑ 상기 암호화된 프로그램이 속하는 패키지에 대응하는 상기 패키지 키를 검색하는 단계와,

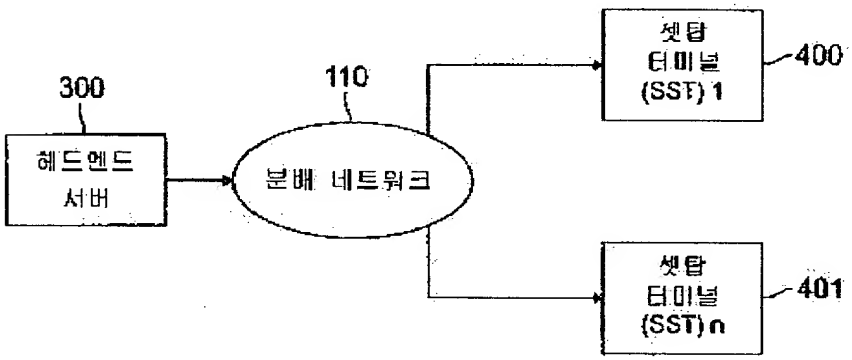
ⓒ 상기 프로그램 키를 획득하기 위하여 상기 검색된 패키지 키를 이용하여 상기 패키지 정보를 암호 해독하는 단계와,

ⓓ 상기 프로그램 키를 이용하여 상기 암호화된 프로그램을 암호 해독하는 단계

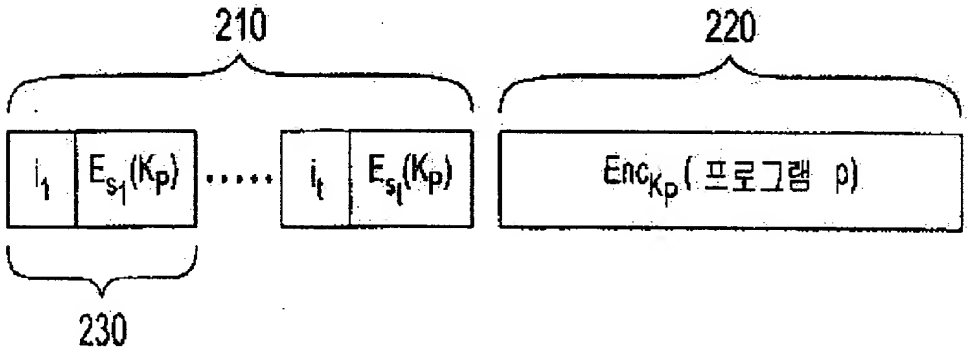
를 포함하는 제조 물품.

도면

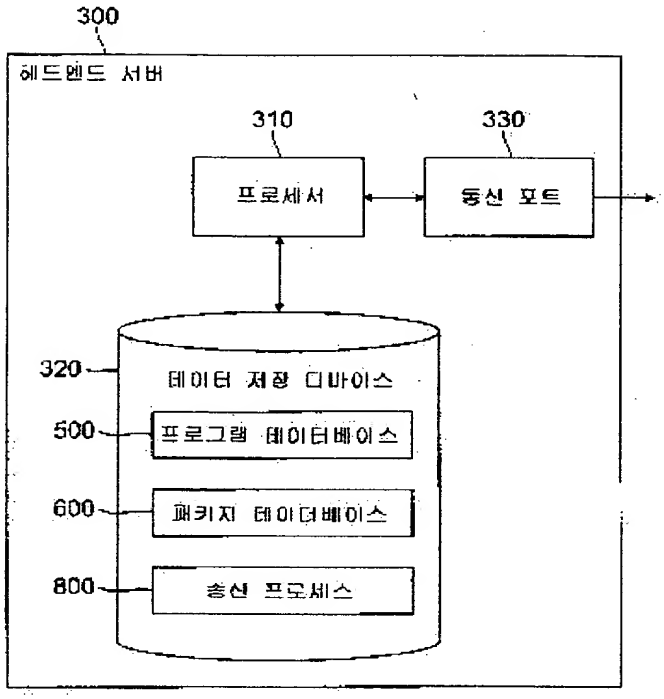
도면1



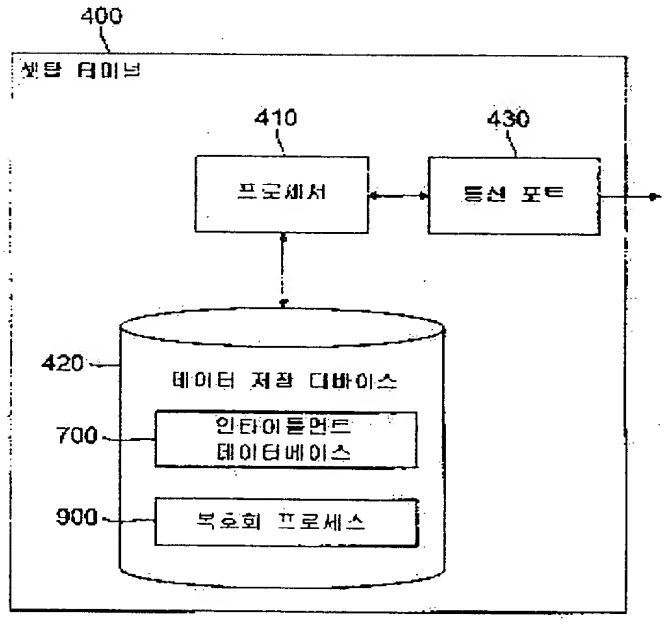
도면2



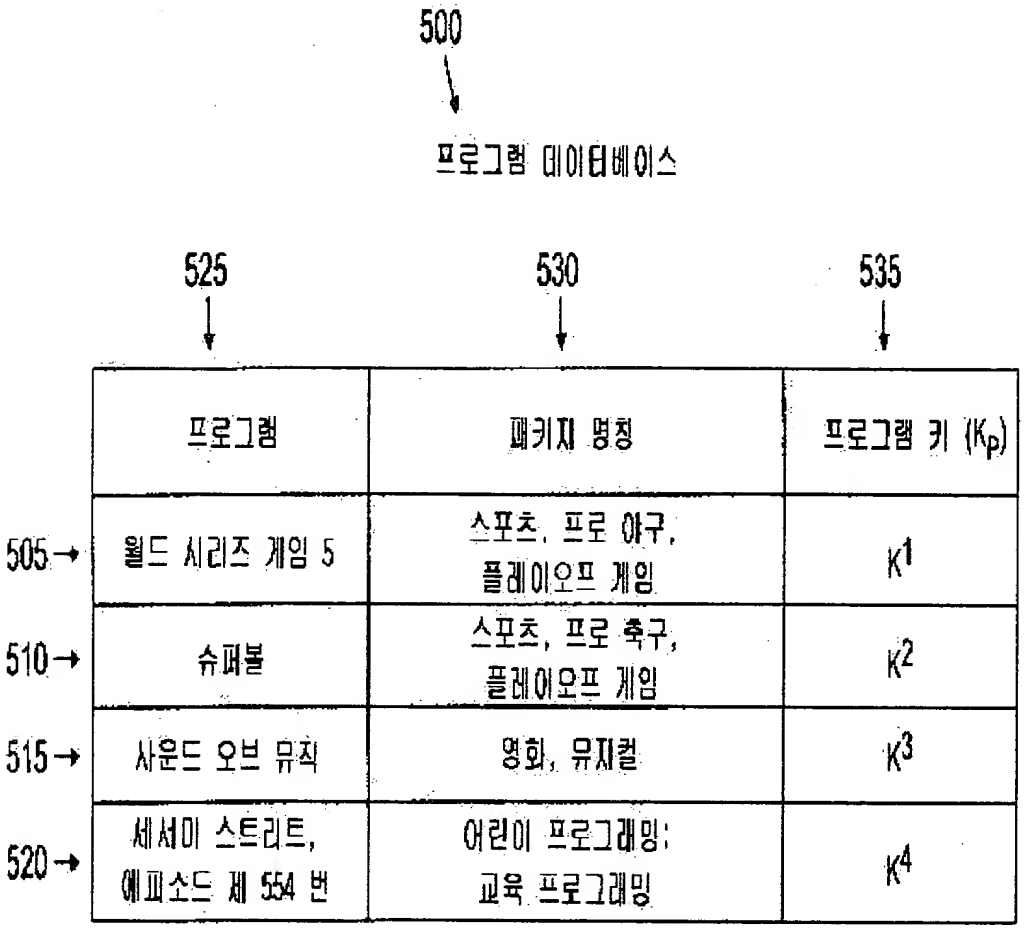
도면3


300
헤드엔드 서버
310
330
프로세서
통신 포트
320
데이터 저장 디바이스
500
프로그램 데이터베이스
600
패키지 데이터베이스
800
송신 프로세스

도면4


400
셋탑 터미널
410
430
프로세서
통신 포트
420
데이터 저장 디바이스
700
인터이틀먼트
데이터베이스
900
복호화 프로세스

도면5



	프로그램	패키지 명칭	프로그램 키 (K_p)
505 →	월드 시리즈 게임 5	스포츠, 프로 야구, 플레이오프 게임	K^1
510 →	슈퍼볼	스포츠, 프로 축구, 플레이오프 게임	K^2
515 →	사운드 오브 뮤직	영화, 뮤지컬	K^3
520 →	세서미 스트리트, 에피소드 제 554 번	어린이 프로그래밍; 교육 프로그래밍	K^4

도면6

600

패키지 데이터베이스

	650 패키지 ID	660 패키지 명칭	670 패키지 키 (S_j)
605 →	0001	스포츠	S^1
610 →	0010	프로 축구	S^2
615 →	0011	프로 야구	S^3
620 →	0100	플레이오프 게임	S^4
625 →	0101	영화	S^5
630 →	0110	뮤지컬	S^6
635 →	0111	어린이 프로그래밍	S^7
640 →	1000	교육 프로그래밍	S^8

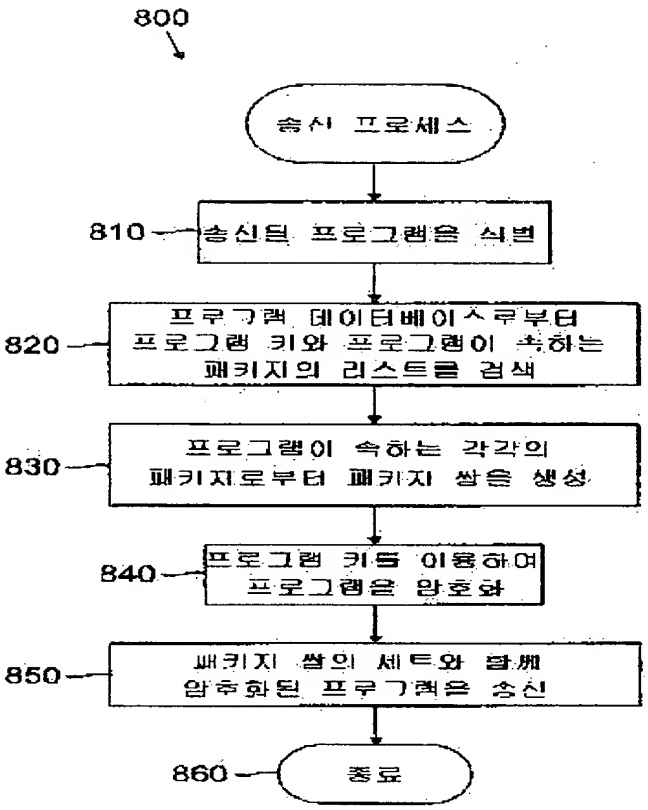
도면7

700

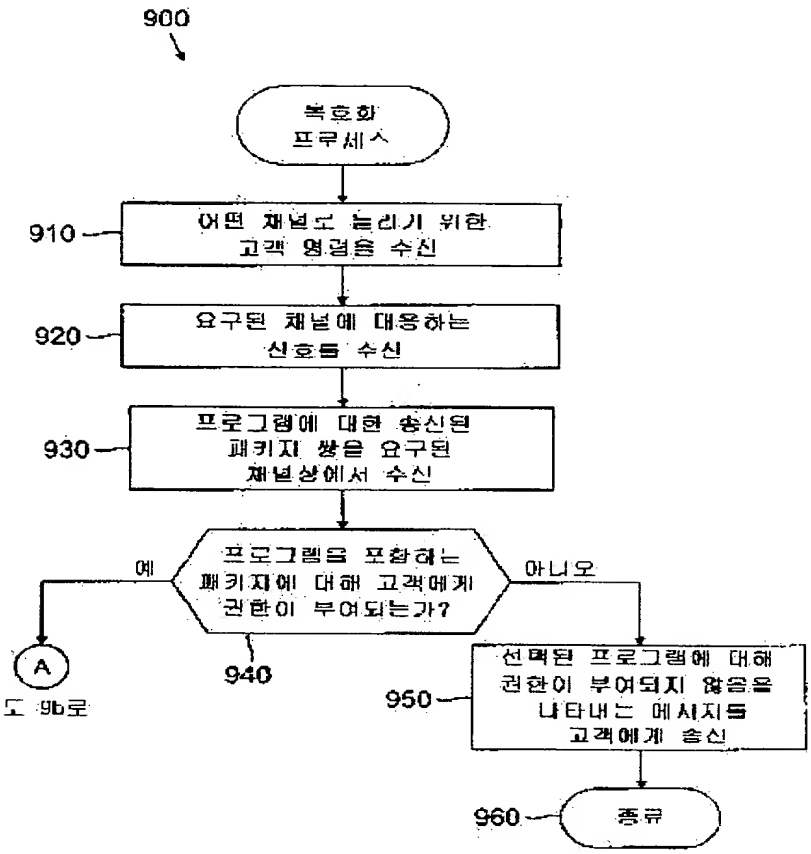
인타이틀먼트 데이터베이스

	725 패키지 ID	735 패키지 키 (S_j)
710 →	0011	S^3
715 →	0100	S^4
720 →	1000	S^8

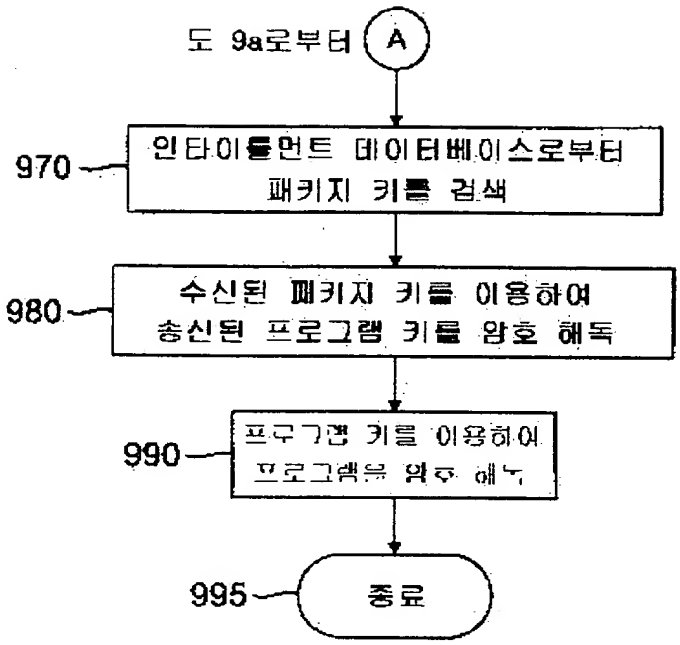
도면8


800
송신 프로세스
810
송신될 프로그램을 식별
820
프로그램 데이터베이스로부터 프로그램 키와 프로그램이 속하는 패키지의 리스트를 검색
830
프로그램이 속하는 각각의 패키지로부터 패키지 쌍을 생성
840
프로그램 키를 이용하여 프로그램을 암호화
850
패키지 쌍의 세트와 함께 암호화된 프로그램을 송신
860
종료

도면9a


900
복호화 프로세스
910
어떤 채널도 듣기 위한 고객 명령을 수신
920
요구된 채널에 대응하는 신호를 수신
930
프로그램에 대한 송신된 패키지 쌍을 요구된 채널상에서 수신
프로그램을 포함하는 패키지에 대해 고객에게 권한이 부여되는가?
예
아니오
940
A
도 9b로
950
선택된 프로그램에 대해 권한이 부여되지 않음을 나타내는 메시지를 고객에게 송신
960
종료

도면9b


도 9a로부터
A
970
인타이틀먼트 데이터베이스로부터
패키지 키를 검색
980
수신된 패키지 키를 이용하여
송신된 프로그램 키를 암호 해독
990
프로그램 키를 이용하여
프로그램을 암호 해독
995
종료